CJIS Technical Audit Checklist

Under the Criminal Justice Information Service (CJIS) Security Policy provisions, the Texas Department of Public Safety (DPS) serves as the CJIS Systems Agency for the State of Texas. Our team of experienced and professional staff is responsible for auditing local agencies to ensure compliance with the technical aspects of the FBI CJIS Division's policies and regulations.

The following list of items and this checklist will need to be emailed to the auditor prior to the agency's scheduled conference call; or the agency will be found non-compliant. Sample policies and editable versions are available at
https://www.dps.texas.gov/section/crime-records-service/cjis-documents
Please ensure the agency modifies the sample policies for the agency's use.

Required documents:

- ☐ Please email a list of any CAD/RMS/JMS/Livescan etc., which contains CJI (If the system contains FBI, SID, NIC#'s etc. in addition to PII, this would be considered CJI). Also include information on where the data is stored – is this an on-site solution or a cloud solution.
- ☐ Awareness Training – AT-1 (Policies and Procedures) If this training is taken somewhere other than CJIS online, we will need verification of training. https://www.cjisonline.com/
- ☐ Incident Response Plan – IR-1 (Policies and Procedures)
- ☐ Access Control – AC-1 (Policies and Procedures)
- ☐ Personnel Sanctions
- ☐ Security Alerts & Advisories policy *** If utilizing sample policy, please remove the line stating "Below is a list of resource samples….." and list only the alerts the agency is actually subscribed to.
- ☐ A roster of employees with agency-issued credentials (ID cards, badges) or authorized personnel (third party vendors) allowed unescorted access into physically secure areas.
- ☐ Media Protection – MP-1 (Policies and Procedures)
- ☐ System Integrity - SI-1 (Policies and Procedures)
- ☐ Current Network Diagram (FIPS Certs., hosted agencies, livescan, backup location, etc.)
- ☐ Physically Secure Location – policy listing security measures in place making the agency a secure location.
- ☐ Standard Operating Procedures (SOP)
- ☐ Windows Updates / Anti-Virus / and Personal Firewall –
  - For all terminals that access/provide access to/store and/or process CJI the agency must:
    - Submit a report listing all applicable nodes are current with Windows Updates, Anti-Virus definition updates, and the Firewall is enabled on MDTs (if applicable)
    - Email three screenshots of the nodes showing the above requirements are being met. And…
  - In addition to the report and the screenshots above, the agency shall provide a letter/email from either the Head of the Agency or the LASO stating the agency has verified all CJI nodes are current on Windows Updates, Anti-Virus definition updates, and if applicable, a local Firewall is enabled on the MDTs.

Required only if applicable:

- ☐ Any Security Addendums the agency may have with 3rd party vendors with access to CJI
- ☐ Event logging (5.4.1.1 & 5.4.1.1.1)
- ☐ Management Control Agreements for technical services
- ☐ MDT/MDC policy
- ☐ A MDT/mobile wireless device list containing (IMEI #, phone#, vendor contact info, etc.)
- ☐ A list of all wireless access points / hotspots providing access to CJI